



## 新 gTLD 计划说明备忘录

### 减少恶意行为

发布日期： 2010 年 11 月 12 日

### 新 gTLD 计划背景信息

ICANN 作为一家致力于协调互联网编址系统的多利益主体非营利性机构，自十年前成立以来，一直将在确保互联网安全和稳定的基础上，推动域名市场的竞争作为其主要使命之一，美国及其他国家/地区的政府都对此表示赞赏。通用顶级域名 (gTLD) 的扩展是互联网编址系统的进一步创新、选择和改变的平台。

在向广泛利益主体（政府、个人、民间团体、商业和知识产权社群以及技术群体）所代表的全球互联网群体的所有社群开展详细而漫长的意见征询之后，ICANN 决定引入新 gTLD。致力于这项工作的还有 ICANN 的政府咨询委员会 (GAC)、网络普通用户咨询委员会 (ALAC)、国家或地区代码域名支持组织 (ccNSO) 以及安全与稳定咨询委员会 (SSAC)。意见征询流程促成新 gTLD 引入政策的出台，这项政策由通用名称支持组织 (GNSO) 于 2007 年制定完成，并于 2008 年 6 月由 ICANN 理事会批准通过。

本说明备忘录是 ICANN 发布的一系列旨在帮助全球互联网群体理解《申请人指南》列出的各项要求和流程的文档的一部分。自 2008 年底以来，ICANN 工作人员一直通过针对《申请人指南》草案及其支持文档开展的一系列公众意见讨论会，与互联网群体分享该计划制定流程的进展情况。我们将对所收集的公众意见进行仔细评估，并据此进一步完善计划。

**请注意，本文档只是讨论草案。由于新 gTLD 计划仍需进一步的意见征询和修订，潜在申请人不应以其中所提议的细节内容为准。**

### 本文主要内容摘要

- 虽然已将有关减少恶意行为的九项建议纳入指南，但实际的实施工作仍在进行当中。
- 本备忘录对一些解决方案进行了详细说明。这些解决方案将通过增加对注册人的保护，确保更安全的环境，以及制定和实施发现和打击潜在恶意行为的方法，给 DNS 环境带来重大改进。

## 总结

ICANN 之前曾发布了本说明备忘录的两个版本，旨在说明《申请人指南》中用于解决新 gTLD 下的潜在恶意行为的九项改进措施。[第一版备忘录](#)发布于 2009 年 10 月 3 日，[第二版备忘录](#)发布于 2010 年 5 月 31 日。

本次更新旨在对这些领域出现的其他实施工作进行说明 — 即使这些建议已被纳入指南中，但实际的实施工作仍在进行中。

本备忘录对一些解决方案进行了详细说明。这些解决方案将通过增加对注册人的保护，确保更安全的环境，以及制定和实施发现和打击潜在恶意行为的方法，给 DNS 环境带来重大改进。ICANN 和机构群体将继续合作，以推出有助于新 gTLD 流程稳定启动的方法和措施。在新 gTLD 计划不断向着启动和实施推进的过程中，安全性、稳定性和灵活性问题仍然是 ICANN 要优先关注的问题。

本文重点讲述了已经出色完成的大量工作，其中大多数工作是由意见征询论坛或工作组中的机构群体志愿者完成的。ICANN 对志愿者所采取的显著改善 DNS 环境的措施表示赞赏和感谢。

《最终申请人指南提案》中目前已包含或引用的九项新 gTLD 实施建议如下：

1. **审核注册管理执行机构** — 这项建议要求适当审查新 gTLD 申请人注册管理执行机构，以确定申请人注册管理执行机构是否有犯罪或恶意行为记录。
2. **DNSSEC 部署示范计划** — 这项建议强制要求新 gTLD 申请人对 DNSSEC 部署计划进行展示说明，以降低伪造 DNS 记录的风险。
3. **禁止使用通配符** — 这项建议要求对 DNS 通配符进行适当控制，降低 DNS 重定向到恶意站点的风险。
4. **删除孤立的粘合记录** — 这项建议要求在 gTLD 中删除某个系统的同时删除名称服务器记录，以降低恶意行为参与者使用这些剩余记录的风险。
5. **要求详细的 WHOIS 记录** — 这项建议要求新 gTLD 提供并维护对“详细的 WHOIS”记录的访问权限，以提高 WHOIS 数据的准确性和完整性。使用详细的 WHOIS 记录在 TLD 内部提供了更加完整的合同链，从而为打击恶意使用新 gTLD 提供了一个重要机制。反过来，在识别出恶意行为时，也能更迅速地进行数据搜索并解决恶意行为。
6. **区域文件的集中访问** — 这项建议要求通过一个集中的来源提供获取注册管理机构区域文件数据的访问凭证，从而能够更加快速准确地确定每个 TLD 中的关键联系点。这样在 TLD 遭受恶意行为时，可以减少采取纠正措施所需的时间。
7. **记录注册管理机构级别的滥用问题联系人和程序** — 这项建议要求 gTLD 建立一个单一联系点来负责处理滥用投诉，并要求注册管理机构对其旨在打击滥用问题的政策进行说明。这些要求被认为是成功打击新 gTLD 中恶意行为的基本步骤。
8. **参与注册管理机构加急安全请求流程** — 这项建议使新 gTLD 能够通过建立专门的流程来审查和批准加急安全请求，从而根据对 DNS 的系统威胁情况采取快速有效的措施。
9. **高安全性区域验证的草案框架** — 这项建议提议创建一个旨在分配 TLD 的志愿计划，希望可以建立并验证更高水平的安全性和信任度。该计划的总体目标是为希望具备优异的安全性和可信度的 TLD 以及将受益于这种优异特性的 TLD 业务模型提供一种机制。

本备忘录的其余部分将说明与各个建议相关的具体工作状态。

## 九种恶意行为建议的状态

本节对减少新 gTLD 中潜在恶意行为的九种建议的现状进行了说明。

### 1 审核注册管理执行机构

- 现状

该建议要求对注册管理执行机构进行“审核”或背景核查，这是改进新 gTLD 申请人的申请流程的指导原则。新 gTLD 申请流程中包含了将新 gTLD 申请人作为申请流程的一部分进行核查的具体标准。已经对《最终申请人指南提案》进行了修订，在意见回应中增加了详细具体的说明。删除了对恐怖主义的具体引用（正如背景核查区域的超简列表）。只在以下两个区域进行背景筛查：一般业务尽职调查和犯罪记录；以及抢注行为记录。

### 2 要求 DNSSEC 部署

- 现状<sup>1</sup>

DNSSEC 部署计划是新 gTLD 申请流程的必备部分，也是每个新 gTLD 授权前测试的组成部分。注册管理机构协议的规定 6 中包含以下条款：“注册管理执行机构应签署实施域名系统安全扩展（简称“DNSSEC”）的 TLD 区域文件。”自从在 2010 年 7 月 15 日签署了 DNSSEC 的根区域以来，已经有 64 个 TLD（截止 2010 年 11 月 11 日）签署了其区域。

### 3 禁止使用通配符

- 现状

与禁止使用 DNS 通配符相关的文字仍然是注册管理机构协议规定 6 的一部分。自从 ICANN 理事会在 2009 年 6 月的悉尼公开会议上决定新顶级域名不得使用 DNS 重定向及合成 DNS 响应以来，尚未对这项禁令进行任何更改。

### 4 孤立的粘合记录

- 现状

SSAC 成立了一个工作组来研究这一问题，并且已经针对 TLD 区域和注册完成了大量分析，以更清楚地了解孤立记录在主要 TLD 中的分布情况。工作组已经审查了当前所有 gTLD 的区域文件，并就孤立记录用于恶意行为的频率进行了分析。SSAC 已经编制了一份工作组报告草案，目前已进入最后的小组审查阶段。由 SSAC 工作组提出的建议可以就如何管理孤立记录为注册管理机构提供额外的指导，并就将其纳入 gTLD 关键流程进行评估。正如 2010 年 9 月 28 日发布的 ICANN 理事会决议 2.8 中所述，“指南中的现有条款要求每个申请人针对管理和删除已从区域中删除的名称的孤立粘合记录提供措施建议。应保留这项要求；如果 SSAC 在其报告中就此项问题提出了新的建议，则将对这一要求进行调整。”

## 5 要求详细的 WHOIS

- 现状

这项建议的状态没有变化，所有新 gTLD 都要求“详细的 WHOIS”。所有新 gTLD 都要根据注册管理机构协议的规定 4 执行详细 WHOIS 要求。有关本建议的更多信息请查阅 2010 年 5 月 30 日发布的 [WHOIS 说明备忘录](#)。

此外，已对《最终申请人指南提案》中的评估和评分系统进行了修订，暂定为那些表示将提供可搜索的 Whois 功能并将获得附加分的申请人纳入附加标准。

## 6 区域文件的集中访问

- 现状

ICANN 接受了创建相应机制以支持区域文件记录的集中访问这一建议，并成立了名为“区域文件访问咨询委员会”(“ZFA AG”)的咨询委员会，其使命是与群体机构共同制定一个提案，旨在创建支持区域文件集中访问的机制。ZFA AG 已完成使命，具体信息可参见 2010 年 5 月 13 日发布的[战略提案](#)。

总体来说，ZFA AG 建议采用混合模式（以下简称“模式”），即结合采用本提案中提到的增强型双边模式和信息交换机构模式。该“模式”为希望访问区域文件的申请人提供单点联系方式，很大程度上保留了数据提供商的现有角色和运营职能。该“模式”为当前区域文件访问系统带来了两个变化。第一，它按以下三个主要类别对区域文件数据提供商（即注册管理执行机构）与消费者（例如，反滥用和商标保护组织、研究人员、学者等）之间的关系进行标准化：申请标准、访问标准和文件/记录格式标准。第二，它引入了轻量级信息交换机构来进行区域文件访问系统的身份管理，以便为希望访问区域文件的消费者提供单点联系方式。

ICANN 正在制定一项计划，旨在为落实本提案中提到的建议确定合适的服务提供商。

可以在注册管理机构协议规定 4 的第 2 节找到对区域文件访问的引用。

## 7 记录注册管理机构级别的滥用问题联系人和政策

- 现状

该建议要求新 gTLD 对具体的注册管理机构滥用问题联系人进行记录，并对具体的反滥用政策进行说明，这也是对所有新 gTLD 的要求。这一建议与原始的恶意行为备忘录中的条款相同，具体条款可查阅第 5 单元的第 5.4.1 节。

## 8 参与注册管理机构加急安全请求 (ERSR) 流程

### • 现状和/或更新

2009 年 10 月 1 日, ICANN [宣布](#)可以使用注册管理机构加急安全请求 (ERSR) 流程。仅在为了避免对 DNS 稳定性或安全性带来不良影响而要求注册管理机构立即采取行动的情况下, gTLD 注册管理机构才使用该流程。

[ERSR](#) 是基于 Web 的提交程序, 由 ICANN 和 gTLD 注册管理机构共同制定, 在以下情况下可以依据这一流程迅速采取行动:

- gTLD 注册管理机构向 ICANN 报告其 TLD 和/或 DNS 目前或即将出现安全问题;
- gTLD 注册管理机构请求对其可能采取或已采取的旨在减少或消除事件的行动进行合同豁免。

合同豁免是指在响应事件所需的时间段内免除遵守注册管理机构协议具体条款的要求。

## 9 高安全性区域验证框架

### • 现状

创建高安全性区域验证草案框架的建议是由银行及金融服务团体 (例如 BITS, 美国某金融服务机构联合会) 提出的, 并实施了名为“高安全性区域顶级域名计划” (简称“HSTLD 计划”) 的措施。该措施旨在起草一份高安全性区域验证控制框架提案。为了对创建该框架以及制定机构群体审核提案的可能方案进行分析, ICANN 成立了高安全性区域顶级域名咨询委员会 (“HSTLD AG”)。HSTLD AG 的使命是与机构群体一起通过自下而上的制定模式, 提出一个包含控制标准和鼓励性措施的志愿计划, 以增强选择参与该计划的 TLD 的安全性和信任度。HSTLD 计划不会由 ICANN 实施, 而是由独立的第三方实体负责, 第三方实体将建立标准并根据这些标准验证 TLD。

2010 年 6 月 16 日, ICANN 发布了 HSTLD AG 的 [HSTLD 速览 #2](#) 以征询公众意见。该速览提供了一个包含原则、标准及控制标准的公共框架, 允许那些希望被指定为高安全性顶级域名的 TLD 注册管理执行机构支持或展示增强的安全措施和政策。现有框架形成了 HSTLD 计划核心要求的基础, 可参考速览中的附录 A。

该速览的公众意见征询期已于 2010 年 7 月 21 日结束, 对公众意见的总结和分析将随同《最终申请人指南提案》一同发布。另外, ICANN 和 HSTLD AG 承认对该计划进行信息征询 (RFI) 是很有意义的。RFI 的目的是帮助 ICANN 机构群体理解基于 HSTLD 标准评估 TLD 注册管理机构的潜在框架和方法, 确定为了确保成功必须对标准草案和整个计划做哪些改进, 并评估 HSTLD 计划提案的可行性。2010 年 9 月 22 日 ICANN [宣布](#)发布 [RFI](#), 意见征询截止日期为 2010 年 11 月 23 日。

2010 年 11 月 23 日 RFI 阶段结束之后, ICANN 和 HSTLD AG 有足够的时间来回答问题、总结并分析这些意见, 然后将制定下一步计划。

ICANN 将继续致力于减少新 gTLD 中的恶意行为, 并支持作为独立运行的志愿计划的 HSTLD 方案的制定。